APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/828,559	04/06/2001	Osamu Shibata	29288.0300	6490

20322   7590   01/24/2008
SNELL & WILMER L.L.P. (Main)
400 EAST VAN BUREN
ONE ARIZONA CENTER
PHOENIX, AZ 85004-2202

EXAMINER
HOMAYOUNMEHR, FARID

ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
01/24/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

PTOL-90A (Rcv. 04/07)

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>30 October 2007</u>.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-50</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-50</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

1.   This action is responsive to amendments filed 10/30/07, the application filed

4/6/2001.

2.   Claims 1-50 are pending in the case.

Response to Arguments

3.   Applicant argues that Ishibashi does not disclose at least three of the aspects of

the claimed invention. The three aspects and the corresponding responses are as

follows:

(1) Applicant argues: "Applicants' content decryption key is generated in a device that uses the

generated content decryption key to decrypt the encrypted content, so the content decryption key

is not required to be transferred to the content decryption device (see, e.g., FIGS. 1, 3-7). In

contrast, Ishibashi's content decryption key is generated in a device that does not use the

generated content decryption key to decrypt the content, so the content decryption key must be

transferred to the appropriate content decryption device (see, e.g; FIGS. 6, 8)". However,

Ishibashi also generates the decryption key at the device that performs decryption.

Example of it is item 100 in fig. 8, where content decryption key Kcd is generated and

used to decrypt the content. Note that in Ishibashi, the content decryption key is not

transferred between the sender and receiver in the clear form. The elements to

generate the key are transferred to the device 100, but not the decryption key in its clear

text form (i.e. without protection by encryption).

(2) Applicant argues: "Applicants' content keys do not need to be encrypted or decrypted

(nowhere in the application do Applicants mention encrypting the content keys, whereas other

items are clearly encrypted and decrypted) because they are not transferred outside the content

encryption/decryption device. In contrast, Ishibashi's content keys must be encrypted and

decrypted because they are transferred outside of the encryption and decryption devices (see,

e.g., col. 3, lines 58-60 and FIGS. 6, 8)". However, as mentioned above, Ishibashi's keys

are not transferred in clear text either. In addition, applicant clearly encrypts and

decrypts the decryption limitations, which are also clearly transferred between the two

parties. The encryption and decryption keys of applicant's invention are clearly

generated based on the decryption limitations. Therefore, similar to Ishibashi,

applicant's keys are generated based on elements that are encrypted and transferred

between the two parties.

(3) Applicant argues: "Applicants' time-varying keys used in mutual authentication are not

transferred between the encryption and decryption devices (see, e.g., FIGS. 1, 3-7). In contrast,

Ishibashi's "session keys" (to which the Examiner compares Applicant's time-varying keys) are

transferred between the encryption and decryption devices (see, e.g., FIGS. 6, 8)." However, as

indicated in the rejection under section 112, the Specification does not explicitly support

a time-varying key that is not transferred between the two parties. Applicant has cited

Figs. 1, 3-7 in support of the new limitation of time-varying keys not transferred between

two parties, but said figures do not explicitly support such limitation. In addition, as

indicated in the new grounds of rejection, using time-varying keys that do not travel

between arties were well-known at the time of invention. For example, the patent to

Frutiger shows that time varying keys synchronized once, are used for generation of

keys at the receiver and sending side.

Applicant also repeats their arguments stated in their previous responses, and argue

that the new limitations such as requiring the **contents** encryption/decryption device are

not disclosed by Ishibashi. However, as indicated in the rejection under section 112, the

Specification does not define a contents encryption/decryption device, that is

distinguished from an encryption/decryption device. Therefore, it is not clear how

requiring a **contents** encryption/decryption device makes the invention distinguishable

over an encryption/decryption device.

Based on the discussion above, applicant's argument relative to allowability of the

pending claims is found non-persuasive.

Claim Rejections - 35 USC § 112

4.   The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly
> claiming the subject matter which the applicant regards as his invention.

5.   Claim 1 recites the limitation "decryption device" in the second to last paragraph.

There is insufficient antecedent basis for this limitation in the claim. The rejection is

applicable to all claims containing the same feature.

6.   The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of
> making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the
> art to which it pertains, or with which it is most nearly connected, to make and use the same and shall
> set forth the best mode contemplated by the inventor of carrying out his invention.

7.   Claims 1-50 rejected under 35 U.S.C. 112, first paragraph, as failing to comply

with the written description requirement. The claim(s) contains subject matter which

was not described in the specification in such a way as to reasonably convey to one

skilled in the relevant art that the inventor(s), at the time the application was filed, had

possession of the claimed invention. The amended clams include three new limitations,

which were not described in the Specification. Applicant does not identify specific

portions of the Specification in support of the said three limitations, and the Examiner is

unable to locate support in the Specification. The three limitations are as follows:

7.1.   The limitation of "contents decryption device" is introduced to replace "decryption

device". Applicant's argument to distinguish their art relies on this new limitation,

however, there is no definition or description of "contents decryption device" that

distinguishes it from the general meaning of the device, which is a device that, among

other potential activities, performs contents decryption.

7.2.   The limitation of "wherein the contents decryption key is not required to be

encrypted or decrypted by the decryption device" is introduced, however, there is no

definition or description of the said limitation in the Specification. First, as mentioned

above, the decryption device lacks antecedent basis. It is not clear if the decryption

device is the same as the "contents decryption device", which is also not described, or it

is a different entity. If it is a different entity, it is not clear how it is different or

distinguished from the contents decryption device. Therefore, it is not clear where the

encrypted decryption key is decrypted, and how it is delivered to the device that

performs contents decryption.

7.3.   The limitation of "time-varying keys not required to be transmitted to the contents

decryption device" is introduced. Applicant's argument to distinguish their art relies on

this new limitation, however, there is no explicit definition or description of "time-varying

keys not required to be transmitted to the contents decryption device". The concept of

synchronized time-varying keys being used to generate a key at the receiver and

transmitter is understood in the prior art. These keys are synchronized once and then

produce synchronized time-varying keys until they need re-synchronization again.

However, applicant's original disclosure provides no detail about time-varying keys not

required to be transmitted to the contents decryption device. Therefore, it is not possible

to see how the new limitation could potentially distinguish the invention from the prior

art.

Claim Rejections - 35 USC § 103

8.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9.   Claim 1 rejected under 35 U.S.C. 103(a) as being unpatentable over Ishibashi

(U.S. Patent No. 6,728,379 B1, filed July 28, 1999).

9.1.   As per claim 1, Ishibashi is directed to a copyright protection system (column 1

line 22 to 25) comprising: a contents encryption device (item 10 and associated text.

Items 100 and 200 also perform encryption) and a contents decryption device

(Information Processors 100 and 200 both perform decryption, e.g. item 136), wherein

cryptographic communication is performed between the contents encryption device and

the contents decryption device (Figures 2 and 3 and the associated texts) using a

contents key (Kce and Kcd as shown in Figures and associated text. Also note that

public key encryption, (which uses separate keys for encryption and decryption) can be

replaced by private (symmetric) key encryption, which uses one key for both encryption

and decryption, as indicated in col. 4 line 34 to 42), wherein the contents encryption

device includes a contents storage section for storing contents (item 11 of Fig. 8 and

associated text), a first contents key generation section for generating the contents key

(item 14 of Fig. 8 and associated text, also see column 4 line 24 to 33) based on a

second decryption limitation obtained by updating a first decryption limitation (column 6

line 1 to 20 discloses SCMS as an example system of a copy control scheme that uses

control codes in set in the content and the associated encryption keys for copy control.

Also note that the process of updating the content key based on the copy control code

and client usage and purchase of content is clearly disclosed in col. 9 line 52 to col. 13

line 60. The process is explained within item 100, but it would have been obvious to a

person skilled in art to perform the same in item 10 (content provider), where the

content key is generated. The motivation is to allow the content provider to control the

copying of the content), and a first encryption section for encrypting the contents using

the contents key (item 13 Fig. 8) and outputting the encrypted contents (item 15 Fig. 8),

and wherein the contents decryption device includes a second contents key generation

section for generating the contents key from the second decryption limitation (item 131

of Fig. 8 generates Kcd, which is used to decrypt the content. As the content was

encrypted based on a copy control scheme, namely SCMS, the copy control code was

updated and embedded in the content or the key (see column 10 line 53 to 66 and also

column 13 line 47 to 60), accordingly) and a first decryption section for decrypting the

encrypted contents using the contents key generated by the second contents key

generation section (item 136 of Fig. 8 and associated text), wherein the contents

decryption key is not required to be encrypted or decrypted by the decryption device per

Fig, 8, item 136 is different from item 131), wherein the contents encryption device

further includes a third encryption section for encrypting the first decryption limitation

using a time-varying key and outputting the second encrypted decryption limitation to

the contents decryption device (the copy control data (encryption limitation) is buried in

content data (see, for example, col. 1 line 1-5), and all the communication between

devices is encrypted by a session key (see, for example, col. 9 line 3-10, or col. 10 line

60 to col. 13 line 47), which is a time-varying key), and the contents decryption device

further includes a third decryption section for decrypting the second encrypted

decryption limitation transferred from the third encryption section using the time-varying

key and outputting the first decryption limitation (all communication is encrypted by a

session key as explained above. Also see Fig. 6 and associated text).

10.   Claims 2-50 rejected under 35 U.S.C. 103(a) as being unpatentable over

Ishibashi (U.S. Patent No. 6,728,379 B1, filed July 28, 1999), and further in view of

Frutiger (US Patent No. 4'071'693, dated 1/31/1978).

10.1. As per claim 2, Ishibashi is directed to a copyright protection system according to

claim 1, wherein the contents decryption device further includes a decryption limitation

updating section for updating the first decryption limitation to the second decryption

limitation in accordance with a decryption limitation updating rule (column 12 line 4 to

15), and a second encryption section for encrypting the second decryption limitation

using a time-varying key (column 12 line 33 to 43), and outputting the first encrypted

decryption limitation, wherein the contents encryption device further includes a second

decryption section for decrypting the first encrypted decryption limitation transferred

from the second encryption section using the time-varying key to generate the second

decryption limitation, wherein the first contents key generation section generates the

contents key based on the second decryption limitation generated by the second

decryption section (column 13 line 15 to 26. Note that the Content provider and the

information system 100 also perform the SCMS method for inclusion of the copy control

code to limit number of allowable copies at item 100. Therefore, content encryption and

key generation at the content provider also involves updating encryption keys based on

the control code and in accordance with the copy rights updated at the information

center).

Ishibashi teaches a time-varying key that is transmitted between the sender and the

receiver, however, it does not explicitly teach time varying keys that are not transmitted

between the two parties. Frutiger teaches time-varying keys generated at the receiver

and transmitter, and used to generate keys used for encryption/decryption (see the

abstract and columns 1 and 2). Ishibashi and Frutiger are analogous art as they are

both directed to systems for secure transmission of data. At the time of invention, it

would have been obvious to the one skilled in art to combine the method of key

generation as taught by Frutiger, in the system of Ishibashi, to include time varying keys

in its method of secure delivery of data. The motivation to do so would be to improve the

security of key exchange between the receiver and transmitter, which is a critical

element of all security systems relying on encryption and decryption keys.

10.2.   As per claim 3, Ishibashi is directed to a copyright protection system according to

claim 2, wherein the contents encryption device further includes a first common key

storage section for storing a common key (column 9 line 4 to 10 discloses a mutual

authentication between all elements in Fig. 8. Furthermore, the said mutual

authentication is described in column 7 lines 33 to 65. Therefore, the content provider

executes a mutual authentication method, namely ISO/IEC 9798-3, which will require

establishment of a common key, and a location for storage), a decryption limitation

storage section for storing the first decryption limitation (as described in response to

claim 2, the content provider performs SCMS in association with the item 100 to

establish a copy code, and therefore stores a copy code, which is updated in sync with

item 100), a first random number generation section for generating a first random

number, a first mutual authentication section for performing mutual authentication in

association with the contents decryption device using the first random number, and a

second random number transferred from the contents decryption device, a first time-

varying key generation section for generating the time-varying key using the first

random number and the second random number in response to the authentication by

the first mutual authentication section (random number generation and exchange

between two parties performing mutual authentication, and establishment of a session

key, are part of a mutual authentication method, namely ISO/IEC 9798-3 performed

between the content provider and item 100, as described in Fig. 6 and the associated

text, and also column 5 lines 5 to 21), and wherein the contents decryption device

further includes a second common key storage section for storing the common key, a

second random number generation section for generating the second random number,

a second mutual authentication section for performing mutual authentication in

association with the contents encryption device using the second random number and

the first random number, a second time-varying key generation section for generating

the time-varying key using the second random number and the first random number in

response to the authentication by the second mutual authentication section (again, item

100 performs SCMS for receiving the copy codes using a session key obtained

thorough a mutual authentication).

10.3.   As per claims 4 and 5 Ishibashi is directed to a copyright protection system

according to claim 1, wherein the contents decryption device further includes a first

decryption limitation updating section for updating the first decryption limitation to the

second decryption limitation in accordance with a decryption limitation updating rule

(column 6 lines 1 to 20), and a second contents key generation section for generating

the contents key based on the second decryption limitation updated by the first

decryption limitation updating section (column 10 line 42 to column 11 line 9), wherein

the contents encryption device further includes a second decryption limitation updating

section for updating the first decryption limitation to the second decryption limitation in

accordance with the decryption limitation updating rule in response to the updating of

the first decryption limitation by the first decryption limitation updating section, the first

contents key generation section generates the contents key based on the second

decryption limitation updated by the first decryption limitation updating section (the

content provider and Information Processing Unit 200 both perform SCMS and

implement copy code updating and secure exchange of the copy code).

10.4. As per claim 6, Ishibashi is directed to a copyright protection system according to

claim 5, wherein the second decryption limitation updating section updates the first

decryption limitation to the second decryption limitation in advance (column 10 lines 9 to

26 discloses the case when the content decryption and distribution decryption keys are

supplied by the Key Distribution Center, item 30, and therefore are supplied in

advanced), the first contents key generation section generates the contents key from

the second decryption limitation, and the second decryption limitation updating section

stores the second decryption limitation in the decryption limitation storage section in

response to the start of processing by the first encryption section (see responses to

claim 3 and 4).

10.5. As per claim 7, Ishibashi is directed to a copyright protection system according to

claim 3, wherein the first and second time-varying key generation sections generate the

time-varying key based on the first and second random numbers and the common key

(time varying keys, and their generation is disclosed in method ISO/IEC 9798-3 for

mutual authentication. See column 7 line 37).

10.6. As per claim 8, Ishibashi is directed to a copyright protection system according to claim 3, wherein the first and second contents key generation sections generate the contents key based on the second decryption limitation and the time-varying key (see response to claims 45 and 5).

10.7. As per claim 9, Ishibashi is directed to a copyright protection system according to claim 3, wherein the contents encryption device and the contents decryption device further include respective first and second data sequence key generation sections for generating a data sequence key based on a data sequence input to or output from the contents encryption device and the contents decryption device, and wherein the first and second time-varying key generation sections generate the time-varying key based on the first and second random numbers and the respective data sequence key(as described in column 13 lines 57 to 60 and column 14 lines 22 to 24, alternative and more comprehensive methods to secure the exchange of keys between the parties may be deployed. Sequence key generation is a well-known method to synchronize receiver and transmitter engaged in secure data transmission and improve the strength of encryption, as described in text books such as Bruce Schneier's Applied Cryptography, ISBN 0-471-11709-9, (see section 9.5). Ishibashi's disclosure of mutual authentication implies use of well-known methods to perform mutual authentication, such as sequence key generation).

10.8. As per claim 10, 11, 12 Ishibashi is directed to a copyright protection system according to claim 3, wherein the contents encryption device and the contents decryption device further include respective first and second data sequence key generation sections for generating a data sequence key based on a data sequence input to or output from the contents encryption device and the contents decryption device, and wherein the first and second time-varying key generation sections generate the time-varying key based on the first and second random numbers, the common key, and the respective data sequence key (see response to claims 9, 3 and 4).

10.9. As per claim 13, Ishibashi is directed to a copyright protection system according to claim 3, wherein the first and second mutual authentication sections mutually authenticate the contents decryption device and the contents encryption device, respectively, by communication in accordance with a challenge-response type authentication protocol (as described in column 13 lines 57 to 60 and column 14 lines 22 to 24, alternative and more comprehensive methods to secure the exchange of keys between the parties may be deployed. Challenge-response is a well-known method to establish mutual authentication between parties, as described in text books such as Bruce Schneier's Applied Cryptography, ISBN 0-471-11709-9, (see section 3.2, page 54). Ishibashi's disclosure of mutual authentication implies use of well-known methods to perform mutual authentication, such as sequence key generation).

10.11. As per claim 14, Ishibashi is directed to an contents encryption device for

performing cryptographic communication in association with a contents decryption

device using a contents key, comprising: a contents storage section for storing contents

(fig. 8 item 11); a second encryption section for encrypting the first decryption limitation

using a time-varying key and outputting the second encrypted decryption limitation to

the contents decryption device (see response to claim 1); a contents key generation

section (item 14) for generating the contents key based on a second decryption

limitation obtained by updating a first decryption limitation (column 6 lines 1 to 20,

column 10 lines 53 to 66, and column 12 lines 25 to 44 disclose Ishibashi's use of

SCMS, which controls the number of copies made from copyright protected material by

updating limitations of copy codes in the content data and keys); and a first encryption

section for encrypting the contents using the contents key and outputting the encrypted

contents (item 16).

10.12. As per claims 15 to 25 Ishibashi is directed to an contents encryption device

according to claim 14 (item 100 in Fig. 8 discloses both encryption and contents

decryption devices, as it receives the encrypted content data from item 10, decrypts it to

extract the content, and re-encrypts it in accordance with the copy control code (copy

limitation) and sends it to item 200 (another Information Center), which perform

decryption. As described in responses to claims 1 to 13, this process is secured by

mutual authentication between items 10, 100, 200 and other elements in Fig. 8. Mutual

authentication involves the use of encryption techniques such as time-varying keys,

random number generation and use for key generation, challenge–response protocol,

data segmentation, etc. Ishibashi also discloses SCMS method for copy control. In the

following, the contents encryption device is disclosed by item 100, and contents

decryption device is disclosed by item 200. Item 100 does disclose all the elements of

claim 14, as it includes and encryption section, and performs SCMS to update the copy

code sent to item 200), further including a decryption section for decrypting the first

encrypted decryption limitation transferred from the contents decryption device (item

131) using the time-varying key to generate the second decryption limitation, and the

contents key generation section generates the contents key based on the second

decryption limitation generated by the contents decryption device (item 133 and the

associated text, also see responses to claims 1 to 14).

10.13. As per claim 26, Ishibashi is directed to a contents decryption device (Fig. 8 item

100 or 200) for performing cryptographic communication in association with an contents

encryption device (item 100 or 10) using a contents key, comprising: a second

decryption section for decrypting a second encrypted decryption limitation transferred

from the contents encryption device using the time-varying key and outputting a first

decryption limitation (see response to claim 1); a decryption limitation updating section

for updating a first decryption limitation to a second decryption limitation in accordance

with a decryption limitation updating rule (the copy control mechanism as discussed in

claim 1 in item 200, which performs SMCS protocol which includes updating a copy

code, as described in column 6 line 1 to 20); a contents key generation section for

generating the contents key from a second decryption limitation (item 231 generates the

key to decrypt the content decryption key, which in accordance with SMCS includes a

copy code (decryption limitation); and a first decryption section for decrypting encrypted

contents using the contents key generated by the contents key generation section (item

236 and the associated text).

10.14. As per claims 27 to 36 Ishibashi is directed to a contents decryption device

according to claim 26, further including an encryption section for encrypting the second

decryption limitation using a time-varying key, and outputting the first encrypted

decryption limitation (item 200 performs SMCS protocol which includes updating a copy

code, as described in column 6 line 1 to 20).

10.15. As per claims 37 to 47, Ishibashi is directed to a recording medium storing a

program for use in causing a computer to perform cryptographic communication with an

contents encryption device (Fig. 8 item 100), a second decryption section for decrypting

a second encrypted decryption limitation transferred from the contents encryption

device using the time-varying key and outputting a first decryption limitation (see

response to claim 1); a decryption limitation updating section for updating a first

decryption limitation to a second decryption limitation in accordance with a decryption

limitation updating rule (the copy control mechanism as discussed in claim 1 in item

200, which performs SMCS protocol which includes updating a copy code, as described

in column 6 line 1 to 20); using a contents key, wherein: the program causes the

computer to function as: a contents key generation section for generating the contents

key from a second decryption limitation (item 133, as described in response to claim

15); and a first decryption section for decrypting encrypted contents using the contents

key generated by the contents key generation section (item 131 as explained in

response to claim 15, and response to claims 1 to 16).

10.16. As per claim 48, Ishibashi is directed to a copyright protection system according

to claim 1, wherein the first and second contents key generation sections generate the

contents key by using an algorithm which uses the second decryption limitation as an

input (as discussed in the Response to Arguments section above, Ishibashi teaches a

key (K_{cd}^{cx}), which is an encryption key generated based on the copy control code

(second decryption limitation). Therefore the content key generator generates the key

with the second decryption limitation as an input).

10.17 As per claim 49, Ishibashi is directed to a copyright protection system according

to claim 48, but Ishibashi does not disclose details such as the encryption technique to

be used to perform different encryption processes, as the details of many encryption

algorithms and techniques were well known in art at the time of his invention. Therefore,

Ishibashi does not explicitly specify the one-way function as the algorithm to perform

encryption.

Examiner takes the official notice that One-way function was a well known and widely

practiced encryption technique at the time of invention. Therefore, it would have been

obvious to the one skilled in art to use the One-way function as the algorithm to

generate the key. The motivation to do so would have been to protect the key

generation algorithm by using a one-way function, which makes it difficult for the

hackers to discover the elements of the key generation process by analyzing the key.

As an example of prior art, please see Applied Cryptography (as identified in response

to claim 9) sections 2.4 and 8.1.

10.18 The requirements of claim 50 is substantially similar to the requirements of

claims 1-49.

Conclusion

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Farid Homayounmehr whose telephone number is 571

272 3739. The examiner can normally be reached on 9 hrs Mon-Fri, off Monday

biweekly.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone

number for the organization where this application or proceeding is assigned is 571-

273-8300.
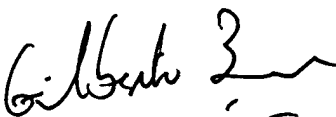
Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Farid Homayounmehr

Examiner

Art Unit: 2132

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100